Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method comprising:

modifying an original header associated with an original data packet wherein key information is added, wherein the modifying an original header further includes identifying at least one field in the original header for transporting packet assembly information and replacing the packet assembly information in the field with at least a portion of the key information;

encrypting original data associated with the original data packet in response to the key information; and

forming an encrypted data packet including [[the]] a modified header and [[the]] encrypted data, wherein the modified header is a same size as the original header.

2. (Previously Presented) The method according to claim 1 further comprising receiving a unique key identifier associated with the encrypted data packet.

3. (Previously Presented) The method according to claim 2 wherein the modifying further comprises modifying the original header in response to the unique key identifier.

4. (Currently Amended) The method according to claim 1 wherein the modifying further comprises replacing [[the]] a fragmentation identification and a fragment offset of the original header with a mixing key and an offset.

5. (Original) The method according to claim 1 wherein the original data packet and the encrypted data packet utilize Internet Protocol version 4.

6. A system comprising:

means for modifying an original header associated with an original data packet wherein key information is added, wherein the means for modifying an original header further includes the means for identifying at least one field in the original header for transporting packet assembly information and replacing the packet assembly information in the field with at least a portion of the key information;

means for encrypting original data associated with the original data packet in response to the key information; and

means for forming an encrypted data packet including [[the]] a modified header and [[the]] encrypted data, wherein the modified header is a same size as the original header.

7-9 (Canceled).

10. (New) A network encryption method, comprising:

receiving a packet having a packet header and a packet payload;

identifying a first field of the packet header for carrying packet assembly information;

replacing the packet assembly information in the first field with a first encryption value and a second encryption value;

encrypting original data associated with the packet payload in response to the first encryption value and the second encryption value; and

forming an encrypted data packet including a modified header and encrypted data, wherein the modified header has a same size as the packet header.

11. (New) The method according to claim 10, further comprising:

identifying a second field of the packet header for carrying packet assembly information; and

replacing the packet assembly information in the second field with a third encryption value.

12. (New) The method according to claim 11, wherein the identifying a first field of the packet header for carrying packet assembly information includes identifying a fragment identification in the packet header.

13. (New) The method according to claim 12, wherein the identifying a second field of the packet header for carrying packet assembly information includes identifying a fragment offset in the packet header.

14. (New) The method according to claim 13, wherein the replacing packet assembly information in the first field with a first encryption value and a second encryption value further includes writing a mixing key refreshing ratio value and a working key refresh ratio in the first field.

15. (New) The method according to claim 14, wherein the replacing packet assembly information in the second field with a third encryption value further includes writing an offset of selecting key value in the second field.

16. (New) The method according to claim 10, further comprising receiving a unique key identifier associated with the encrypted data packet.

17. (New) The method according to claim 10, wherein the packet and the encrypted data packet utilize Internet Protocol version 4.

18. (New) The method according to claim 11, further includes activating checksum in accordance with a checksum field in the packet header after the packet assembly information in the first and the second fields is replaced with the first, second, and third encryption values.